Toyama Math. J.
Vol. 34(2011), 1-22

Lupe Latin squares of order odd, 3-odd, A^2+3B^2 with $\gcm(A,B)=1$

Kazuo Azukawa

Abstract. Let p be an odd integer which is written as $p = A^2 + 3B^2$ with $\gcm(A,B) = 1$ and which is non-divisible by 3. We define $(1,3)$-Lupe and $(3,1)$-Lupe properties of a Latin p-square or a magic p-square. For any such p, we construct complete Latin p-squares N_+^+, N_-^+ of $(1,3)$-Lupe property, and N_+^-, N_-^- of $(3,1)$-Lupe property. We show that the products $N_+^+ \times N_-^+$ and $N_+^- \times N_-^-$ are Euler squares, so that $pN_+^+ + N_-^+$ and $N_+^+ + pN_-^+$ (resp. $pN_+^- + N_-^-$ and $N_+^- + pN_-^-$) are complete magic squares of $(1,3)$-Lupe property (resp. $(3,1)$-Lupe property).

1. Odd and 3-odd numbers A^2+3B^2 with $\gcm(A,B)=1$

We start with the following lemma:

Lemma 1. *If $A, B \in \mathbf{N}$ and $\gcm(A,B) = 1$, then there exist unique $(a,b),(a',b') \in \{0,\dots,A\}\times\{0,\dots,B\}\backslash\{(0,0),(A,B)\}$ such that $bA-aB = 1$ and $b'A-a'B = -1$. For these it holds that $(a,b)+(a',b') = (A,B)$.*

Proof. To prove the existence, let

$$\frac{B}{A} = a_0 + \frac{1}{a_1+}\,\frac{1}{a_2+}\,\cdots\,\frac{1}{a_{n-1}+}\,\frac{1}{a_n}$$

be the continued fraction expansion of the number B/A such that $a_0 \in \{0\}\cup\mathbf{N}$, $a_j \in \mathbf{N} (n \geq j \geq 1)$ and that $a_n \geq 2$ whenever $n \geq 1$. Let

$$\frac{y}{x} = a_0 + \frac{1}{a_1+}\,\frac{1}{a_2+}\,\cdots\,\frac{1}{a_{n-2}+}\,\frac{1}{a_{n-1}}$$

with $x, y \in \mathbf{Z}, x \geq 0, \mathrm{gcm}(x, y) = 1$ (when $n = 0$, $(x, y) = (0, 1)$)(cf. [A-Y]). Then, $(x, y) \in \{0, \ldots, A-1\} \times \{0, \ldots, B\} \backslash \{(0, 0)\}$ and $yA - xB = (-1)^n$; furthermore if $(x', y') := (A - x, B - y)$, then $(x', y') \in \{1, \ldots, A\} \times \{0, \ldots, B\} \backslash \{(A, B)\}$ and $y'A - x'B = (-1)^{n+1}$. If n is even (resp. odd), then $(a, b) = (x, y), (a', b') = (x', y')$ (resp. $(a, b) = (x', y'), (a', b') = (x, y)$) have the desired properties. The uniqueness and the latter half of the assertions are easy to prove.

From now on we assume that $p \in \mathbf{N}$ and $(A, B) \in \mathbf{N}^2$ satisfy

$$p = A^2 + 3B^2, \tag{1}$$

$$\mathrm{gcm}(A, B) = 1, \tag{2}$$

$$p \text{ is odd}, \tag{3}$$

$$p \text{ is not divisible by 3}. \tag{4}$$

We may call property (4) p being 3-**odd**. Take $(a, b), (a', b') \in \{0, \ldots, A\} \times \{0, \ldots, B\} \backslash \{(0, 0), (A, B)\}$ satisfying

$$bA - aB = 1 \text{ and} \tag{5}$$

$$b'A - a'B = -1 \tag{6}$$

as in Lemma 1 and set

$$q := aA + 3bB, \quad q' := a'A + 3b'B. \tag{7}$$

We note that

$$q + q' = p, \tag{8}$$

$$qA = ap + 3B, \quad qB = bp - A, \tag{9}$$

$$q'A = a'p - 3B, \quad q'B = b'p + A. \tag{10}$$

It follows from (1),(2),and (3) that

$$A+B \text{ is odd;} \tag{11}$$

especially

$$A \neq B. \tag{12}$$

Lemma 2. *Let p, A, B satisfy* (1)-(4) *and q, q' be defined by* (7). *Then* $\gcm(q,p)=1$ *and* $\gcm(q',p)=1$.

Proof. It follows from (1) and (4) that A is not divisible by 3, so that $\gcm(A,3B)=1$ by (2). Take $\ell, m \in \mathbf{Z}$ such that $\ell A + m3B = 1$. It follows from (9) that $\ell(bp-qB)+m(qA-ap)=1$, so that $(-\ell B+mA)q+(\ell b-ma)p=1$; therefore, $\gcm(q,p)=1$. Since $q'=p-q$ by (8), $\gcm(q',p)=\gcm(p-q,p)=\gcm(q,p)=1$, as desired.

Lemma 3. *Let p, a, b, q, q' be as in Lemma 2. Then*

$$p(a^2+3b^2)-q^2=3, \quad p(a'^2+3b'^2)-q'^2=3, \tag{13}$$

$$qq' \equiv 3 \pmod{p}. \tag{14}$$

Proof. The identity

$$(A^2+3B^2)(x^2+3y^2)=(xA+3yB)^2+3(yA-xB)^2$$

implies (13). It follows from (8) and (13) that $qq'=q(p-q)\equiv -q^2 \equiv 3 \pmod{p}$, as desired.

Remark 4. It is well known that for every $p \in \mathbf{N}$,which is odd and 3-odd, the following seven statements are mutually equivalent(cf. [H]):
(i) There exists $(A,B) \in \mathbf{N}^2$ such that $p=A^2+3B^2$ with $\gcm(A,B)=1$.
(ii) There exists $(X,Y) \in \mathbf{N}^2$ such that $p=X^2+Y^2+XY$ with $\gcm(X,Y)=1$.
(iii) There exists $q \in \mathbf{N}$ such that $q^2 \equiv -3 \pmod{p}$.
(iv) For every prime p' with $p'|p$, it holds that $p' \equiv 1 \pmod{3}$.

(v) For every prime p' with $p'|p$, there exists $(A, B) \in \mathbf{N}^2$ such that $p' = A^2 + 3B^2$ with $\gcm(A, B) = 1$.
(vi) For every prime p' with $p'|p$, there exists $(X, Y) \in \mathbf{N}^2$ such that $p' = X^2 + Y^2 + XY$with $\gcm(X, Y) = 1$.
(vii) For every prime p' with $p'|p$, there exists $q \in \mathbf{N}$ such that $q^2 \equiv -3 \pmod{p'}$.

A proof of implication (i)⇒(iii) has been given in the proof of Lemma 3.

From (iv), every p satisfying one of (i)-(vii), $p \equiv 1 \pmod 3$.

For completeness we shall prove the equivalence of (i) and (ii), so that of (v) and (vi). We first note the following:
If $p = A^2 + 3B^2, A, B \in \mathbf{N}$, then $p = (A + B)^2 + 2B(B - A)$, so that

$$2|p \quad \Leftrightarrow \quad 2|(A + B); \quad \text{and}$$

$$3|p \quad \Leftrightarrow \quad 3|A.$$

If $p = X^2 + Y^2 + XY,\ X, Y \in \mathbf{N}$, then $p = (X - Y)^2 + 3XY$, so that

$$2|p \quad \Leftrightarrow \quad 2|X \text{ and } 2|Y; \quad \text{and}$$

$$3|p \quad \Leftrightarrow \quad 3|(X - Y).$$

Set

$$E_1 := \{(X, Y) \in \mathbf{N}^2 | X \text{ is odd},\ Y \text{ is even}\},$$

$$E_2 := \{(X, Y) \in \mathbf{N}^2 | X, Y \text{ are odd},\ Y > X\},$$

and $E := E_1 \cup E_2$. Set

$$F_1 = \{(A, B) \in \mathbf{N}^2 | A + B \text{ is odd},\ A > B\},$$

$$F_2 = \{(A, B) \in \mathbf{N}^2 | A + B \text{ is odd},\ A < B\},$$

and $F := F_1 \cup F_2$. Then the set

$$\{p = X^2 + Y^2 + XY | X, Y \in \mathbf{N}, X \neq Y,\ p \text{ is odd}\}$$

is uniquely parametrized by E, and the set

$$\{p = A^2 + 3B^2 | A, B \in \mathbf{N}, p \text{ is odd}\}$$

is by F. Let $\Phi : E \to F$ be defined by

$$E_1 \ni (X,Y) \mapsto (X+Y/2, Y/2) \in F_1,$$

$$E_2 \ni (X,Y) \mapsto ((Y-X)/2, (Y+X)/2) \in F_2,$$

and $\Psi : F \to E$ be by

$$F_1 \ni (A,B) \mapsto (A-B, 2B) \in E_1,$$

$$F_2 \ni (A,B) \mapsto (B-A, A+B) \in E_2.$$

Then, $\Phi \circ \Psi = \mathrm{id}_F$ and $\Psi \circ \Phi = \mathrm{id}_E$. Furthermore, if $\Phi(X,Y) = (A,B)$, then

$$3|(X-Y) \quad \Leftrightarrow \quad 3|A; \quad \text{and}$$

$$\gcm(X,Y) = 1 \quad \Leftrightarrow \quad \gcm(A,B) = 1.$$

This proves the equivalence of (i) and (ii).

A typical example of numbers satisfying (ii) is the **hex numbers** $h_n := n^2+(n+1)^2+n(n+1) = 3n^2+3n+1 = (n+1)^3-n^3$ $(n=1,2,\ldots)$.

2. Constructions of N_+^+ and N_-^+

Let $\ell \in \mathbf{N}$. For $\alpha \in \mathbf{Z}$, let $r_\ell(\alpha)$ denote the remainder of α divided by ℓ; therefore, $r_\ell(\alpha) \in \{0,1,\ldots,\ell-1\}$. For $\alpha, \beta \in \mathbf{Z}$ with $\alpha < \beta$, define

$$[\alpha,\beta]_\ell := \{r_\ell(i) | i = \alpha, \alpha+1, \ldots, \beta\}.$$

Especially, $[1,\ell]_\ell = \{0,1,\ldots,\ell-1\}$. An ℓ-square matrix M with entries in a set X is considered as a mapping from $[1,\ell]_\ell^2$ into X, and written as $M = (M_{ij})_{(i,j)\in[1,\ell]_\ell^2} = (M_{ij})_{i,j}$. We also write $M_{ij} = M(i,j)$.

Definitions. (i) For an integer $\ell \geq 3$, a **Latin** (resp. **magic**) ℓ**-square** is an ℓ-square matrix $[1,\ell]_\ell^2 \to [1,\ell]_\ell$ (resp. an ℓ-square bijective matrix $[1,\ell]_\ell^2 \to [1,\ell^2]_{\ell^2}$) whose restrictions to all rows and all columns are surjective (resp. are of sum $m_\ell := \ell(\ell^2-1)/2$).
(ii) A Latin (resp. magic) ℓ-square is called **complete** if all 2ℓ general

diagonals are also surjective (resp. are also of sum m_ℓ).

Now, let p, A, B satisfying (1)-(4) be fixed. Let $(a,b),(a',b') \in \{0,\dots,A\}\times\{0,\dots,B\}\backslash\{(0,0),(A,B)\}$ satisfy (5),(6), and q, q' be given by (7). Let N_+^+(resp. N_-^+, N_+^-, and N_-^-) $:[1,p]_p^2 \to [1,p]_p$ be defined by

$$(N_+^+)_{ij} := r_p(iq+j) \quad \text{(resp.} \tag{15}$$

$$(N_-^+)_{ij} := r_p(iq'+j), \tag{16}$$

$$(N_+^-)_{ij} := r_p(iq+3j), \quad \text{and} \tag{17}$$

$$(N_-^-)_{ij} := r_p(iq'+3j)). \tag{18}$$

Lemma 5. *Assume $A > B$. If*

$$P = [0,A-1]_p^2, \quad Q = [0,B-1]_p \times [A, A+3B-1]_p,$$

then the image $N_+^+(P\cup Q) = [1,p]_p$.

Proof. As in the proof of Proposition 5 in [A], we consider an auxiliary matrix $L = (L_{ij})_{ij} : [0,A]_{A+B} \times [0,a+b-1]_{A+B} \to [1,A+B]_{A+B}$, defined by

$$L_{ij} := r_{A+B}(i(a+b)+j) \tag{19}$$

for $(i,j) \in [0,A]_{A+B} \times [0,a+b-1]_{A+B}$. It follows from

$$A(a+b) - a(A+B) = 1 \tag{20}$$

that for $j = 0,\dots,a+b-2$,

$$L_{Aj} = L_{0,j+1}. \tag{21}$$

Set

$$\ell := (r_{A+B}(0), r_{A+B}(a+b), \dots, r_{A+B}((A-1)(a+b))),$$

$$s := (r_{A+B}(A(a+b)), r_{A+B}((A+1)(a+b)), \ldots, r_{A+B}((A+B-1)(a+b))).$$

Because of (20), we have

$$(\text{Image } \ell) \cup (\text{Image } s) = \{0, 1, \ldots A+B-1\},$$

$$r_{A+B}(A(a+b)) = 1, \quad \text{and}$$

$$s = (r_{A+B}(1), r_{A+B}((a+b)+1), \ldots, r_{A+B}((B-1)(a+b)+1)).$$

By (19), ${}^t(\ell, r_{A+B}(A(a+b)))$ coincides with the first column of L, and ${}^t s$ coincides with the first B components of the second column of L. We call the numbers in ℓ are of **long label** and in s of **short label**. Let L' be the restriction of L to the set $[0, A-1]_{A+B} \times [0, a+b-1]_{A+B}$. It follows from (19) and (20) that

$$(22) \qquad \begin{cases} \text{in every row of } L', \text{ except the last one, there are} \\ a \ \text{ numbers of long label and } b \ \text{ numbers of short label.} \end{cases}$$

The last row of L' have $a+1$ numbers of long label, $b-1$ numbers of short label and its final component is of long label. For details refer the proof of Proposition 5 in [A]. We construct vectors $\ell_0, \ell_1, \ldots, \ell_{A+B-1}$ inductively as follows: set $\ell_0 := (0, 1, \ldots, A-1)$; constructed $\ell_j = (\ldots, u)$, we set

$$\ell_{j+1} := \begin{cases} (u+1, u+2, \ldots, u+3B), & j+1 \text{ is of short label} \\ (u+1, u+2, \ldots, u+A), & j+1 \text{ is of long label.} \end{cases}$$

Because of $A^2+3B^2 = p$ we have $\ell_{A+B-1} = (\cdots, p-1)$. It follows that, for every $j \in \{0, 1, \ldots, (A+1)(a+b)-2\}$, if $\ell_{r_{A+B}(j)} = (\ldots, u)$, then $\ell_{r_{A+B}(j+1)} = (r_p(u+1), \ldots)$. It follows from (22) that among $\ell_0, \ldots, \ell_{a+b-1}$, we have a long vectors and b short ones, so that $\ell_{a+b-1} = (\ldots, q-1)$. Hence, $\ell_{a+b} = (q, \ldots)$. Inductively, we have $\ell_{r_{A+B}(j(a+b)-1)} = (\ldots, r_p(jq-1))$, $\ell_{r_{A+B}(j(a+b))} = (r_p(jq), \ldots)$, for $j = 1, \ldots, A-1$, so that the matrix

$$\begin{bmatrix} \ell_0 & \ell_1 & \cdots & \ell_{a+b-1} \\ \ell_{r_{A+B}(a+b)} & \ell_{r_{A+B}(a+b+1)} & \cdots & \ell_{r_{A+B}(2(a+b)-1)} \\ \vdots & \vdots & \ddots & \vdots \\ \ell_{r_{A+B}((A-1)(a+b))} & \ell_{r_{A+B}((A-1)(a+b)+1)} & \cdots & \ell^*_{r_{A+B}(A(a+b)-1)} \end{bmatrix}$$

coincides with $N_+^+|_{[0,A-1]_p\times[0,q-1]_p}$, where $\ell^*_{r_{A+B}(A(a+b)-1)}$ is $\ell_0|_{[0,3B-1]_p}$ if $A \geq 3B$, and is $(\ell_0, \ell_1|_{[0,3B-A-1]_p})$ if $A < 3B$ (by (20), $r_{A+B}(A(a+b)-1) = 0$). It follows that

$$N_+^+|_P = {}^t(\ell_{r_{A+B}(0)}, \ell_{r_{A+B}(a+b)}, \ldots, \ell_{r_{A+B}((A-1)(a+b))})$$

and

$$N_+^+|_Q = {}^t(\ell_{r_{A+B}(1)}, \ell_{r_{A+B}(a+b+1)}, \ldots, \ell_{r_{A+B}((B-1)(a+b)+1)}).$$

Since the union of

$$\{r_{A+B}(0), r_{A+B}(a+b), \ldots, r_{A+B}((A-1)(a+b))\} \quad \text{and}$$

$$\{r_{A+B}(1), r_{A+B}((a+b)+1), \ldots, r_{A+B}((B-1)(a+b)+1)\}$$

coincides with

$$(\text{Image } \ell) \cup (\text{Image } s) = \{0, 1, \ldots, A+B-1\},$$

it follows that

$$N_+^+(P \cup Q) = \bigcup_{j=0}^{A+B-1} \text{Image } \ell_j = \{0, \ldots, p-1\},$$

as desired.

Lemma 6. *Assume $B > A$. If*

$$Q = [0, B-1]_p \times [0, 3B-1]_p, \quad P = [0, A-1]_p \times [3B, 3B+A-1]_p,$$

then the image $N_-^+(P \cup Q) = [1, p]_p$.

Proof. Let a matrix $L : [0, B]_{A+B} \times [0, a'+b'-1]_{A+B} \to [1, A+B]_{A+B}$ be defined by

$$L_{ij} := r_{A+B}(i(a'+b')+j) \tag{23}$$

for $(i, j) \in [0, B]_{A+B} \times [0, a'+b'-1]_{A+B}$. Since

$$-b'(B+A) + B(a'+b') = 1 \tag{24}$$

we have for $j=0,\dots,a'+b'-2$,

$$L_{Bj}=L_{0,j+1}. \tag{25}$$

Set

$$\ell:=(r_{A+B}(0),r_{A+B}(a'+b'),\dots,r_{A+B}((B-1)(a'+b'))),$$

$$s:=(r_{A+B}(B(a'+b')),r_{A+B}((B+1)(a'+b')),\dots,r_{A+B}((B+A-1)(a'+b'))).$$

By (24),

$$(\text{Image }\ell)\cup(\text{Image }s)=\{0,1,\dots A+B-1\},$$

$$r_{A+B}(B(a'+b'))=1,\quad \text{and}$$

$$s=(r_{A+B}(1),r_{A+B}((a'+b')+1),\dots,r_{A+B}((A-1)(a'+b')+1)).$$

By (23), ${}^t(\ell,r_{A+B}(B(a'+b')))$ coincides with the first column of L, and ${}^ts$ coincides with the first A components of the second column of L. As before we call the numbers in ℓ are of **long label** and in s of **short label**. Let L' be the restriction of L to the set $[0,B-1]_{A+B}\times[0,a'+b'-1]_{A+B}$. We have

$$\begin{cases}\text{in every row of } L', \text{ except the last one, there are}\\ b' \text{ numbers of long label and } a' \text{ numbers of short label.}\end{cases} \tag{26}$$

As before, we set $\ell_0:=(0,1,\dots,3B-1)$. Constructed $\ell_j=(\dots,u)$, we set

$$\ell_{j+1}:=\begin{cases}(u+1,u+2,\dots,u+A), & j+1 \text{ is of short label}\\ (u+1,u+2,\dots,u+3B), & j+1 \text{ is of long label}\end{cases}$$

for $j=0,\dots,A+B-2$, so that $\ell_{A+B-1}=(\cdots,p-1)$. It follows from (26) that among $\ell_0,\dots,\ell_{a'+b'-1}$, we have b' long vectors and a' short ones, so that $\ell_{a'+b'-1}=(\dots,q'-1)$, and $\ell_{a'+b'}=(q',\dots)$. Hence $\ell_{r_{A+B}(j(a'+b')-1)}=(\dots,r_p(jq'-1))$, $\ell_{r_{A+B}(j(a'+b'))}=(r_p(jq'),\dots)$, for $j=1,\dots,B-1$. As before, we have

$$N_-^+|_Q={}^t(\ell_{r_{A+B}(0)},\ell_{r_{A+B}(a'+b')},\dots,\ell_{r_{A+B}((B-1)(a'+b'))})$$

and

$$N_-^+|_P={}^t(\ell_{r_{A+B}(1)},\ell_{r_{A+B}(a'+b'+1)},\dots,\ell_{r_{A+B}((A-1)(a'+b')+1)}).$$

Since the union of

$$\{r_{A+B}(0), r_{A+B}(a'+b'), \ldots, r_{A+B}((B-1)(a'+b'))\} \quad \text{and}$$

$$\{r_{A+B}(1), r_{A+B}((a'+b')+1), \ldots, r_{A+B}((A-1)(a'+b')+1)\}$$

coincides with

$$(\text{Image } \ell) \cup (\text{Image } s) = \{0, 1, \ldots, A+B-1\},$$

we have

$$N_-^+(P \cup Q) = \bigcup_{j=0}^{A+B-1} \text{Image } \ell_j = \{0, \ldots, p-1\},$$

as desired.

For $(u, v) \in \mathbf{Z}^2$, we denote by $T_{(u,v)}$ the (u, v)-**translation** of the space $[1, p]_p^2$, that is $[1, p]_p^2 \ni (i, j) \mapsto (r_p(i+u), r_p(j+v)) \in [1, p]_p^2$.

Lemma 7.*Let $D \subset [1, p]_p^2$ with* Card $D = p$. *For $(u, v) \in \mathbf{Z}^2$, set $T := T_{(u,v)}$. Let N be one of $N_+^+, N_-^+, N_+^-, N_-^-$.*
If $N(D) = [1, p]_p$, then $N(T(D)) = [1, p]_p$.

Proof. We have

$$\begin{aligned}(N_+^+)_{T(i,j)} - (N_+^+)_{ij} &= r_p(r_p(i+u)q + r_p(j+v)) - r_p(iq+j) \\ &\equiv (i+u)q + (j+v) - (iq+j) \pmod p \\ &\equiv uq + v.\end{aligned}$$

Hence

$$(N_+^+)_{T(i,j)} = r_p((N_+^+)_{ij} + uq + v),$$

so that

$$\begin{aligned}N_+^+(T(D)) &= \{(N_+^+)_{k\ell} | (k, \ell) \in T(D)\} \\ &= \{(N_+^+)_{T(i,j)} | (i, j) \in D\} \\ &= \{r_p((N_+^+)_{ij} + uq + v) | (i, j) \in D\} \\ &= r_p(\{(N_+^+)_{ij} | (i, j) \in D\} + uq + v)\end{aligned}$$

$$\begin{aligned} &= r_p([1,p]_p + uq + v) \\ &= r_p(\{i+uq+v | i \in [1,p]_p\}) \\ &= [1,p]_p. \end{aligned}$$

The assertion for N_+^+ has been proved. Similarly, we have

$$(N_-^+)_{T(i,j)} = r_p((N_-^+)_{ij} + uq' + v),$$

$$(N_+^-)_{T(i,j)} = r_p((N_+^-)_{ij} + uq + 3v),$$

$$(N_-^-)_{T(i,j)} = r_p((N_-^-)_{ij} + uq' + 3v).$$

From these, the assertions for N_-^+, N_+^-, N_-^- follow.

Lemma 8. *Assume $B > A$. If*

$$Q = [0, B-1]_p \times [0, 3B-1]_p, \quad P = [B-A, B-1]_p \times [3B, 3B+A-1]_p,$$

then the image $N_+^+(P \cup Q) = [1,p]_p$.

Proof. By Lemma 7, to prove the assertion, we may show that if

$$Q' = [1, B]_p \times [0, 3B-1]_p, \quad P' = [B-A+1, B]_p \times [3B, 3B+A-1]_p$$

then $N_+^+(P' \cup Q') = [1,p]_p$. Let $R_0 : [1,p]_p^2 \to [1,p]_p^2$ be the transformation given by

$$[1,p]_p^2 \ni (i,j) \mapsto (r_p(p-i), j) \in [1,p]_p^2. \tag{27}$$

Let CP be the cut-and-paste between the first row and the remainder of the space $[1,p]_p^2$, that is $[1,p]_p^2 \ni (i,j) \mapsto (r_p(i-1), j) \in [1,p]_p^2$, and R be the reflection of the space $[1,p]_p^2$ w.r.t. the center row of that space, that is $[1,p]_p^2 \ni (i,j) \mapsto (p-1-i, j) \in [1,p]_p^2$. Since $R_0 = R \circ CP$, the geometry of the transformations CR and R implies $R_0(Q' \cup P') = Q_0 \cup P_0$, where

$$Q_0 = [p-B, p-1]_p \times [0, 3B-1]_p, \; P_0 = [p-B, p-B+A-1]_p \times [3B, 3B+A-1]_p.$$

Since $R_0 \circ R_0 = \mathrm{id}$,

$$Q' \cup P' = R_0(Q_0 \cup P_0). \tag{28}$$

If

$$\overline{N_+^+} := N_+^+ \circ R_0, \tag{29}$$

then in view of definitions (15),(16), and (27) we have

$$\overline{N_+^+} = N_-^+. \tag{30}$$

It follows from (28),(29),(30) that

$$N_+^+(Q' \cup P') = N_+^+(R_0(Q_0 \cup P_0)) = N_-^+(Q_0 \cup P_0). \tag{31}$$

If

$$Q_1 = [0, B-1]_p \times [0, 3B-1]_p, \quad P_1 = [0, A-1]_p \times [3B, 3B+A-1]_p,$$

then Lemma 6 implies $N_-^+(Q_1 \cup P_1) = [1,p]_p$. Since $Q_0 \cup P_0$ is a translation of $Q_1 \cup P_1$, Lemma 7 implies $N_-^+(Q_0 \cup P_0) = [1,p]_p$; combining (31) we have $N_+^+(Q' \cup P') = [1,p]_p$, as desired.

Lemma 9. *Assume $A > B$. If*

$$P = [0, A-1]_p^2, \quad Q = [A-B, A-1]_p \times [A, A+3B-1]_p,$$

then the image $N_-^+(P \cup Q) = [1,p]_p$.

Proof. By Lemma 7, we may show that if

$$P' = [1, A]_p \times [0, A-1]_p, \quad Q' = [A-B+1, A]_p \times [A, A+3B-1]_p,$$

then $N_-^+(P' \cup Q') = [1,p]_p$. As in the proof of Lemma 8, if

$$P_0 = [p-A, p-1]_p \times [0, A-1]_p, \quad Q_0 = [p-A, p-A+B-1]_p \times [A, A+3B-1]_p,$$

then $N_-^+(P' \cup Q') = N_+^+(P_0 \cup Q_0)$. If

$$P_1 = [0, A-1]_p^2, \quad Q_1 = [0, B-1]_p \times [A, A+3B-1]_p,$$

then $P_0 \cup Q_0$ is a translation of $P_1 \cup Q_1$; therefore Lemma 5 implies $N_-^+(P' \cup Q') = N_+^+(P_1 \cup Q_1) = [1,p]_p$, as desired.

Lemma 10. *We have:*

$$N_+^+ \circ T_{(-A,3B)} = N_+^+, \quad N_+^+ \circ T_{(B,A)} = N_+^+; \tag{32}$$

$$N_-^+ \circ T_{(-B,A)} = N_-^+, \quad N_-^+ \circ T_{(A,3B)} = N_-^+. \tag{33}$$

Proof. By (9) we have $qA \equiv 3B,\ qB \equiv -A \pmod p$, so that (32) follows. In fact,

$$N_+^+ \circ T_{(-A,3B)}(i,j) = r_p(q(i-A)+j+3B) = r_p(qi+j) = N_+^+(i,j),$$

etc. By (10) we have $q'A \equiv -3B,\ q'B \equiv A \pmod p$, so that (33) follows. q.e.d.

Proposition 11. *If*

$$P = [0,A-1]_p^2, \quad Q = [0,B-1]_p \times [A,A+3B-1]_p,$$

then $N_+^+(P \cup Q) = [1,p]_p$.

Proof. When $A > B$, the assertion is Lemma 5. Assume $A < B$. By Lemma 8, combining Lemma 7 we have $N_+^+(P' \cup Q) = [1,p]_p$, where

$$P' = [B-A,B-1]_p \times [A+3B, A+3B+A-1]_p.$$

Since $P' = T_{(-A,3B)} \circ T_{(B,A)}(P)$, (32) implies $N_+^+(P \cup Q) = N_+^+(P' \cup Q) = [1,p]_p$, as desired.

Proposition 12. *If*

$$P = [0,A-1]_p^2, \quad Q = [A-B,A-1]_p \times [A,A+3B-1]_p,$$

then $N_-^+(P \cup Q) = [1,p]_p$.

Proof. When $B < A$, the assertion is Lemma 9. Assume $B > A$. By Lemma 6 combining Lemma 7 we get $N_-^+(P \cup Q') = [1,p]_p$, where

$$Q' = [0,B-1]_p \times [p-3B, p-1]_p.$$

Since $Q = T_{(-B,A)} \circ T_{(A,3B)}(Q')$, (33) implies $N_-^+(P \cup Q) = N_-^+(P \cup Q') = [1,p]_p$, as desired.

3. Lupe properties of Latin squares and magic squares

Let p, A, B, a, b, a', b', q, and q' be as in the preceding section. Set

$$d := \frac{p-(A+B)}{2} = \frac{A^2+3B^2-(A+B)}{2} = \frac{A(A-1)}{2}+B^2+\frac{B(B-1)}{2} \in \mathbf{N},$$

and $d' := d - B$.

Definition. A pair (P, Q) of an A-square

$$P = [\alpha, \alpha + A - 1]_p \times [\beta, \beta + A - 1]_p$$

and a $(B, 3B)$-rectangle

$$Q = [\gamma, \gamma + B - 1]_p \times [\delta, \delta + 3B - 1]_p$$

(resp. $(3B, B)$-rectangle

$$Q = [\gamma, \gamma + 3B - 1]_p \times [\delta, \delta + B - 1]_p)$$

in $[1, p]_p^2$ is called $(A, (B, 3B))$-**antipodal** (resp. $(A, (3B, B))$-**antipodal**) if

$$\gamma - \alpha \equiv A + d, \quad \delta - \beta \equiv A + d' (\mathrm{mod}\ p)$$

(resp.

$$\gamma - \alpha \equiv A + d', \ \delta - \beta \equiv A + d (\mathrm{mod}\ p)),$$

that is if the bidistance between P and Q is (d, d') (resp. (d', d)).

Definition. A p-square matrix $M : [1, p]_p^2 \to [1, p]_p$ is called of $(1, 3)$-**Lupe** (resp. $(3, 1)$-**Lupe**) **property** if for any $(A, (B, 3B))$-antipodal (resp. $(A, (3B, B))$-antipodal) pair (P, Q) in $[1, p]_p^2$, the restriction of M to $P \cup Q$ is surjection.

A square matrix $M : [1, p]_p^2 \to [1, p^2]_{p^2}$ is called of $(1, 3)$-**Lupe** (resp. $(3, 1)$-**Lupe**) **property** if for any $(A, (B, 3B))$-antipodal (resp. $(A, (3B, B))$-antipodal) pair (P, Q) in $[1, p]_p^2$, the restriction of M to $P \cup Q$ possesses the sum $m_p = p(p^2 - 1)/2$.

We note that for a p-square matrix $M : [1,p]_p^2 \to [1,p]_p$ or $M : [1,p]_p^2 \to [1,p^2]_{p^2}$, M is of $(1,3)$-Lupe property if and only if ${}^tM$ is of $(3,1)$-Lupe property.

Lemma 13. *It holds that* $(q+1)d \equiv -2B, \quad (q'+1)d \equiv -A+B \pmod{p}$.

Proof. By definition of d as well as (9), we have

$$\begin{aligned}(q+1)d &= \frac{1}{2}(q+1)(p-(A+B)) \\ &= \frac{1}{2}((q+1)p - q(A+B) - (A+B)) \\ &= \frac{1}{2}((q+1)p - (ap+3B+bp-A) - (A+B)) \\ &= -2B + \frac{1}{2}(q+1-(a+b))p,\end{aligned}$$

so that $2((q+1)d+2B) = (q+1-(a+b))p$. Since $\gcm(p,2)=1$, $2|(q+1-(a+b))$. It follows that $(q+1)d \equiv -2B \pmod{p}$. Similarly, using (10) we have

$$\begin{aligned}(q'+1)d &= \frac{1}{2}(q'+1)(p-(A+B)) \\ &= B - A + \frac{1}{2}(q'+1-(a'+b'))p,\end{aligned}$$

so that $2((q'+1)d - B + A) = (q'+1-(a'+b'))p$. Similar argument implies $2|(q'+1-(a'+b'))$, so that $(q'+1)d \equiv -A+B \pmod{p}$, as desired.

Lemma 14. *It holds that*

$$\begin{aligned}&\gcm(q+1,p)=1, \quad &&\gcm(q'+1,p)=1; \\ &\gcm(q-1,p)=1, \quad &&\gcm(q'-1,p)=1; \\ &\gcm(q+3,p)=1, \quad &&\gcm(q'+3,p)=1; \\ &\gcm(q-3,p)=1, \quad &&\gcm(q'-3,p)=1.\end{aligned}$$

Proof. By (9) we have

$$(q+1)A \equiv 3B + A \pmod{p}, \tag{34}$$

$$(q+1)B \equiv B - A \pmod{p}. \tag{35}$$

Since

$$\begin{aligned} \gcm(3B+A, B-A) &= \gcm(4B, B-A) \\ &= \gcm(B, B-A) \text{ (because } B-A \text{ is odd)} \\ &= \gcm(B, -A) \\ &= \gcm(A, B) = 1, \end{aligned}$$

there exist $\ell, m \in \mathbf{Z}$ such that $\ell(3B+A) + m(B-A) = 1$. Substituting (34), (35), we have

$$\ell(q+1)A + m(q+1)B \equiv 1 \pmod{p}.$$

It follows that $\gcm(q+1, p) = 1$.

By (10) we have

$$(q'+1)A \equiv -3B + A, \quad (q'+1)B \equiv A + B \pmod{p}.$$

Since

$$\begin{aligned} \gcm(-3B+A, A+B) &= \gcm(-4B, A+B) \\ &= \gcm(B, A+B) \text{ (because } A+B \text{ is odd)} \\ &= \gcm(A, B) = 1, \end{aligned}$$

similar argument as in the first part implies $\gcm(q'+1, p) = 1$.

By (9) we have

$$(q+3)A \equiv 3(A+B), \quad (q+3)B \equiv -A + 3B \pmod{p}.$$

Since

$$\begin{aligned} \gcm(3(A+B), -A+3B) &= \gcm(3(A+B), -4A) \\ &= \gcm(3(A+B), A) \text{ (because } 3(A+B) \text{ is odd)} \\ &= \gcm(A+B, A) \text{ (because } A \text{ is 3-odd)} \\ &= \gcm(A, B) = 1, \end{aligned}$$

similarly we have $\mathrm{gcm}(q+3,p)=1$

By (10) we have

$$(q'+3)A \equiv 3(A-B), \quad (q'+3)B \equiv A+3B \pmod{p}.$$

Since

$$\begin{aligned}\mathrm{gcm}(3(A-B),A+3B) &= \mathrm{gcm}(4A,A+3B)\\ &= \mathrm{gcm}(A,A+3B) \text{ (because } A+3B \text{ is odd)}\\ &= \mathrm{gcm}(A,3B)\\ &= \mathrm{gcm}(A,B)=1 \text{ (because } A \text{ is 3-odd)},\end{aligned}$$

similarly we have $\mathrm{gcm}(q'+3,p)=1$.

The other four assertions follow from the facts

$$q-1 \equiv -(q'+1), \quad q'-1 \equiv -(q+1), \quad q-3 \equiv -(q'+3), \quad q'-3 \equiv -(q+3) \pmod{p}$$

and the first four results, as desired.

Proposition 15. *The p-squares $N_+^+, N_-^+, N_+^-, N_-^-$ are complete Latin.*

Proof. Since $\mathrm{gcm}(q,p)=1$, $\mathrm{gcm}(q',p)=1$, and $\mathrm{gcm}(3,p)=1$, definitions (15)-(18) imply that $N_+^+, N_-^+, N_+^-, N_-^-$ are Latin squares.
Since for $i,j \in [1,p]_p$ it holds that

$$\begin{aligned}(N_+^+)_{i,r_p(i+j)} &= r_p(iq+(i+j)) = r_p(i(q+1)+j),\\ (N_-^+)_{i,r_p(i+j)} &= r_p(iq'+(i+j)) = r_p(i(q'+1)+j),\\ (N_+^-)_{i,r_p(i+j)} &= r_p(iq+3(i+j)) = r_p(i(q+3)+3j),\\ (N_-^-)_{i,r_p(i+j)} &= r_p(iq'+3(i+j)) = r_p(i(q'+3)+3j),\\ (N_+^+)_{i,r_p(-i+j)} &= r_p(iq+(-i+j)) = r_p(i(q-1)+j),\\ (N_-^+)_{i,r_p(-i+j)} &= r_p(iq'+(-i+j)) = r_p(i(q'-1)+j),\\ (N_+^-)_{i,r_p(-i+j)} &= r_p(iq+3(-i+j)) = r_p(i(q-3)+3j),\\ (N_-^-)_{i,r_p(-i+j)} &= r_p(iq'+3(-i+j)) = r_p(i(q'-3)+3j),\end{aligned}$$

Lemma 14 implies that $N_+^+, N_-^+, N_+^-, N_-^-$ are complete. q.e.d.

Proposition 16. *The p-squares N_+^+, N_-^+ are of $(1,3)$-Lupe property.*

Proof. By virtue of Lemma 7, to prove $(1,3)$-Lupe property of $N := N_+^+$ or N_-^+ we may show that if

$$P = [0, A-1]_p^2, \quad Q = [A+d, A+d+B-1]_p \times [A+d', A+d'+3B-1]_p,$$

then $N(P \cup Q) = [1,p]_p$.

By Proposition 11, if

$$Q_1 = [0, B-1]_p \times [A, A+3B-1]_p,$$

then $N(P \cup Q_1) = [1,p]_p$. We note that $Q = T_{(d+A,d-B)}(Q_1)$. We also note that $N_+^+ \circ T_{(d+A,d-B)} = N_+^+$. In fact,

$$\begin{aligned} N_+^+ \circ T_{(d+A,d-B)}(i,j) - N_+^+(i,j) &= r_p(q(i+d+A)+(j+d-B)) - r_p(qi+j) \\ &= r_p(q(d+A)+d-B) \\ &= r_p(d(q+1)+Aq-B) \\ &= r_p(-2B+3B-B) = 0. \end{aligned}$$

It follows that

$$N_+^+(Q_1) = N_+^+ \circ T_{(d+A,d-B)}(Q_1) = N_+^+(Q).$$

Thus,

$$N_+^+(P \cup Q) = N_+^+(P) \cup N_+^+(Q) = N_+^+(P) \cup N_+^+(Q_1) = N_+^+(P \cup Q_1) = [1,p]_p.$$

On the other hand, by Proposition 12 if

$$Q_2 = [A-B, A-1]_p \times [A, A+3B-1]_p,$$

then $N(P \cup Q_2) = [1,p]_p$. We note that $Q = T_{(d+B,d-B)}(Q_2)$. We also note that $N_-^+ \circ T_{(d+B,d-B)} = N_-^+$. In fact,

$$\begin{aligned} N_-^+ \circ T_{(d+B,d-B)}(i,j) - N_-^+(i,j) &= r_p(q'(i+d+B)+(j+d-B)) - r_p(q'i+j) \\ &= r_p(q'(d+B)+d-B) \\ &= r_p(d(q'+1)+Bq'-B) \\ &= r_p((-A+B)+A-B) = 0. \end{aligned}$$

It follows that

$$N_-^+(Q_2) = N_-^+ \circ T_{(d+B,d-B)}(Q_2) = N_-^+(Q).$$

Thus,

$$N_-^+(P \cup Q) = N_-^+(P) \cup N_-^+(Q) = N_-^+(P) \cup N_-^+(Q_2) = N_-^+(P \cup Q_2) = [1,p]_p,$$

as desired.

Because of $\gcm(q,p)=1,\ \gcm(q',p)=1$, the functions $y, y' : [1,p]_p \to [1,p]_p$ defined by

$$y(j) := r_p(jq), \tag{36}$$

$$y'(j) := r_p(jq') \tag{37}$$

are permutations on $[1,p]_p$.

Proposition 17. *If y, y' are the permutations defined by* (36), (37), *then* $y' \circ N_+^+ = {}^tN_-, \quad y \circ N_-^+ = {}^tN_+^-$.

Proof. We have

$$\begin{aligned} y' \circ N_+^+(i,j) &= y'(r_p(iq+j)) \\ &= r_p((iq+j)q') \\ &= r_p(iqq'+jq') \\ &= r_p(3i+jq') \text{ (by (14))} \\ &= {}^t(N_-^-)(i,j). \end{aligned}$$

Similarly, we have

$$\begin{aligned} y \circ N_-^+(i,j) &= y(r_p(iq'+j)) \\ &= r_p((iq'+j)q) \\ &= r_p(iqq'+jq) \\ &= r_p(3i+jq) \text{ (by (14))} \\ &= {}^t(N_+^-)(i,j), \end{aligned}$$

as desired.

Proposition 18. *The p-squares $N_+^-,\ N_-^-$ possess $(3,1)$-Lupe property.*

Proof. By Proposition 16, the p-squares $y' \circ N_+^+,\ y \circ N_-^+$ possess (1,3)-Lupe property, so that by Proposition 17, the p-squares $N_-^-,\ N_+^-$ possess (3,1)-Lupe property.

Proposition 19. *The product*

$$N_+^+ \times N_-^+ := ([1,p]_p^2 \ni (i,j) \mapsto (N_+^+(i,j), N_-^+(i,j)) \in [1,p]_p^2)$$

is an Euler square, that is $\mathrm{Image}(N_+^+ \times N_-^+) = [1,p]_p^2$.

Proof. Let $i \in [1,p]_p$. Then for $j \in [1,p]_p$, we have

$$N_+^+(i,j) = 0 \Leftrightarrow qi + j \equiv 0 \pmod p \Leftrightarrow j \equiv -qi \pmod p \Leftrightarrow j \equiv q'i \pmod p.$$

Then, $N_+^+(i,q'i) = 0$ and $N_-^+(i,q'i) = r_p(2q'i)$. Since p is odd, $\mathrm{gcm}(2q',p) = \mathrm{gcm}(q',p) = 1$, so that

$$\{(N_+^+ \times N_-^+)(i,iq') | i \in [1,p]_p\} = \{0\} \times [1,p]_p.$$

For $v \in [1,p]_p$, we have

$$N_+^+(i,iq'+v) = r_p(N_+^+(i,iq') + v) = v,$$

$$N_-^+(i,iq'+v) = r_p(N_-^+(i,iq') + v) = r_p(2q'i + v).$$

Thus,

$$\{(N_+^+ \times N_-^+)(i,iq'+v) | i \in [1,p]_p\} = \{v\} \times [1,p]_p,$$

so that $\mathrm{Image}(N_+^+ \times N_-^+)$ contains

$$\bigcup_{v \in [1,p]_p} (\{v\} \times [1,p]_p) = [1,p]_p^2,$$

as desired.

Proposition 20. *The product $N_+^- \times N_-^-$ is an Euler square.*

Proof. Let $j \in [1,p]_p$. For $i \in [1,p]_p$, we have

$$\begin{aligned} N_+^-(i,j)=0 &\Leftrightarrow qi+3j \equiv 0 \pmod p \\ &\Leftrightarrow q(i-qj) \equiv 0 \pmod p \text{ (by (13))} \\ &\Leftrightarrow i \equiv qj \pmod p \text{ (by } \gcm(q,p)=1). \end{aligned}$$

For $v \in [1,p]_p$, it follows that

$$N_+^-(qj+v,j) = N_+^-(qj,j) + r_p(vq) = r_p(vq),$$

$$N_-^-(qj+v,j) = r_p((qj+v)q'+3j) = r_p(6j+vq').$$

Since $\gcm(6,p)=1$, it follows that

$$\{(N_+^- \times N_-^-)(qj+v,j) | j \in [1,p]_p\} = \{r_p(vq)\} \times [1,p]_p.$$

It follows that $\text{Image}(N_+^- \times N_-^-)$ contains

$$\bigcup_{v \in [1,p]_p} (\{r_p(vq)\} \times [1,p]_p) = [1,p]_p^2,$$

as desired.

Theorem 21. *Let $\theta, \psi : [1,p]_p \to [1,p]_p$ be permutations with $\theta(0) = 0, \psi(0) = 0$. If $N_+^+, N_-^+ : [1,p]_p^2 \to [1,p]_p$ are defined by*

$$(N_+^+)_{ij} := \theta(r_p(iq+j)),$$

$$(N_-^+)_{ij} := \psi(r_p(iq'+j)),$$

then the p-squares $pN_+^+ + N_-^+$ and $N_+^+ + pN_-^+$ are complete p-magic squares of $(1,3)$-Lupe property.
If $N_+^-, N_-^- : [1,p]_p^2 \to [1,p]_p$ are defined by

$$(N_+^-)_{ij} := \theta(r_p(iq+3j)),$$

$$(N_-^-)_{ij} := \psi(r_p(iq'+3j)),$$

then the p-squares $pN_+^- + N_-^-$ *and* $N_+^- + pN_-^-$ *are complete p-magic squares of* $(3,1)$*-Lupe property.*

Proof. Set $M^+ := pN_+^+ + N_-^+$ or $:= N_+^+ + pN_-^+$, and $M^- := pN_+^- + N_-^-$ or $:= N_+^- + pN_-^-$. By Proposition 19 combining Proposition 15, M^+ becomes a complete magic square. Proposition 20 as well as Proposition 15 implies that M^- becomes a complete magic square. By Proposition 16 M^+ is of $(1,3)$-Lupe property and by Proposition 18 M^- is of $(3,1)$-Lupe property. The proof is complete.

References

[A] Azukawa, K., *Construction of Lupe magic squares*, Toyama Math. J., **28**(2005), 139–151.

[A-Y] Azukawa, K. and Yuzawa, T., *A remark on the continued fraction expansion of conjugates of the golden section*, Math. J. Toyama Univ., **13**(1990), 165–176.

[H] Hua, L. K., Introduction to Number Theory, Springer-Verlag, Berlin-Heidelberg-New York, **1982**.

Department of Mathematics
University of Toyama
Gofuku, Toyama 930-8555
JAPAN
Email: azuk@sci.u-toyama.ac.jp

(Received November 4, 2010)